Counting & Generating Irreducible Quadratics over $\mathbb{Z}_n[x]$

Robyn Hearn

Department of Mathematics, Simon Fraser University

Introduction

It is known that there are $\binom{p^k}{2}$ irreducible, quadratic, monic polynomials in $\mathrm{GF}(p^k)[x]$ where p is a prime and $k \in \mathbb{N}$. My research began with two questions.

- How many are there in $\mathbb{Z}_n[x]$ for any integer n?
- How can we efficiently generate these polynomials?

Example: Quadratics over $\mathbb{Z}_4$

Reducible			Irreducible
x^2	$=$	$(x+0)^2 = (x+2)^2$	x^2+1
x^2+x	$=$	$(x+0)(x+1)$	x^2+3
x^2+2x	$=$	$(x+0)(x+2)$	x^2+x+1
x^2+3x	$=$	$(x+0)(x+3)$	x^2+x+3
x^2+2x+1	$=$	$(x+1)^2 = (x+3)^2$	x^2+2x+2
x^2+3x+2	$=$	$(x+1)(x+2)$	x^2+2x+3
x^2+3	$=$	$(x+1)(x+3)$	x^2+3x+1
x^2+x+2	$=$	$(x+2)(x+3)$	x^2+3x+3

We may have expected to find $\binom{2^2}{2} = 6$ irreducible quadratics, but in fact there are 8.

Computational Experiments

Let $C(n)$ be the number of irreducible, quadratic, monic polynomials in $\mathbb{Z}_n[x]$.
Using Algorithm 1 coded in C, we found the following.

Sample Data from Algorithm 1

i	$C(2^i)$	$C(3^i)$	$C(5^i)$	$C(7^i)$
1	1	3	10	21
2	8	45	350	1323
3	36	432	9000	65856
4	160	4050	227500	3241350
5	656	36693	5693750	158876571

Conjecture

Let p be an odd prime and $k \in \mathbb{N}$. Then

$$C(2^k) = \begin{cases} \frac{1}{3}2^{2k+1} - \frac{4}{6}2^k & \text{if } k \text{ is even} \\ \frac{1}{3}2^{2k+1} - \frac{5}{6}2^k & \text{if } k \text{ is odd} \end{cases}$$

$$C(p^k) = \begin{cases} p^{2k} - \frac{p^k(p^{k+1}+p+2)}{2(p+1)} & \text{if } k \text{ is even} \\ p^{2k} - \frac{p^k(p^{k+1}+2p+1)}{2(p+1)} & \text{if } k \text{ is odd} \end{cases}$$

Next we wanted to prove this conjecture, determine a general formula, and write an efficient algorithm to generate irreducible quadratics.

Proof Approach

Consider the quadratic, monic polynomials in $\mathbb{Z}_n[x]$. We have

$$n^2 = C(n) + R(n)$$

where $R(n)$ is the number of reducible.
Then $R(n)$ is equal to the number of integer pairs (b, c) such that $0 \le b, c < n$ and

$$x^2 + bx + c \equiv 0 \pmod{n}$$

has a solution.
From Nagell, we see that this congruence has a solution if and only if the following system of congruences, has a solution.

$$y^2 \equiv b^2 - 4c \pmod{4n} \qquad (1)$$

$$y \equiv b \pmod{2} \qquad (2)$$

Congruence (1) suggests that solving for $R(n)$ and $C(n)$ begins by counting squares in $\mathbb{Z}_{4n}$

Counting $R(n)$

We use the following 3 observations from Stangl to count squares in $\mathbb{Z}_{p^i}$ where p is a prime and $i \ge 3$ an integer.

- Let $S(n)$ is the number of squares in $\mathbb{Z}_n$ and $Q(n)$ the number of quadratic residues in $\mathbb{Z}_n$.
$$S(p^i) = Q(p^i) + S(p^{i-2})$$
- If p is an odd prime, then
$$Q(p^i) = \frac{\phi(p^i)}{2} = \frac{p^i - p^{i-1}}{2}$$
- For $p = 2$ we have
$$Q(2^i) = \frac{2^{i-1}}{4} = 2^{i-3}$$

Finally, by the previous congruences and the Chinese Remainder Theorem,

$$R(n) = \frac{n}{2} S(2^{\alpha_0+2}) \Pi_{i=1}^{k} S(p_i^{\alpha_i})$$

when n has prime factorization

$$n = p_0^{\alpha_0} \times p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$$

Main Theorem

Suppose n has prime factorization

$$n = 2^{\alpha_0} \times p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k}$$

where p_i are odd primes and α_i are non-negative integers.
Then the number of irreducible, quadratic, monic polynomials in $\mathbb{Z}_n[x]$ is

$$C(n) = n^2 - \frac{n}{2} S(2^{\alpha_0+2}) \Pi_{i=1}^{k} S(p_i^{\alpha_i})$$

where

$$S(p^i) = \begin{cases} \frac{p^{i+1}+p+2}{2(p+1)} & \text{if } i \text{ is even} \\ \frac{p^{i+1}+2p+1}{2(p+1)} & \text{if } i \text{ is odd} \end{cases} \qquad S(2^i) = \begin{cases} \frac{2^{i-1}+4}{3} & \text{if } i \text{ is even} \\ \frac{2^{i-1}+5}{3} & \text{if } i \text{ is odd} \end{cases}$$

when p is an odd prime.

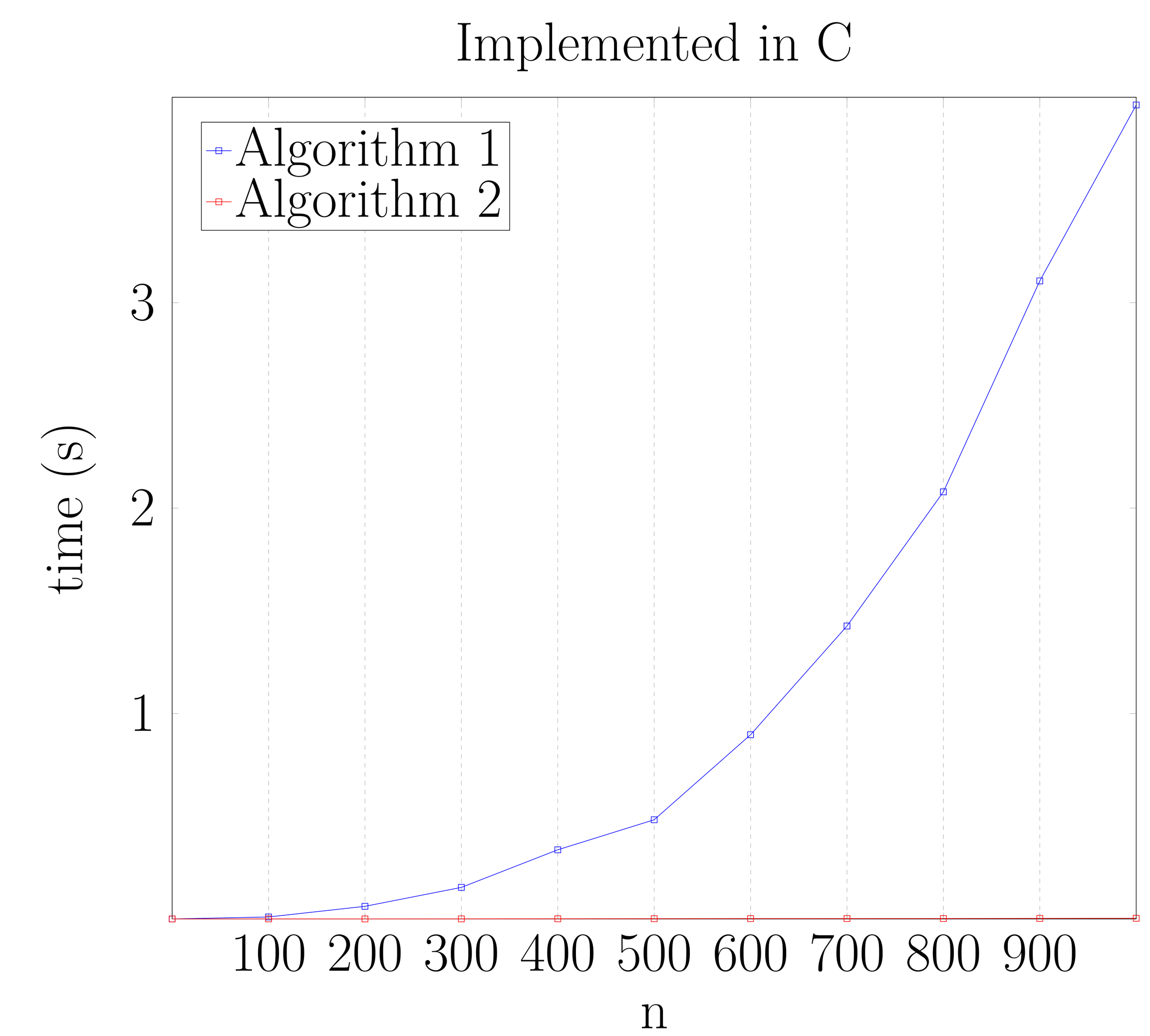
Generating Reducible Quadratics

Algorithm 1

```
P ← []; i ← 0
for b ∈ Z_{p^k} do
  for c ∈ Z_{p^k} do
    for x_0 ∈ Z_{p^k} do
      if x_0^2 + b x_0 + c ≡ 0 (mod p^k) then
        P[i] ← {x^2 + bx + c}; i++
        break
      end if
    end for
  end for
end for
return P
```

Algorithm 2

```
P ← []; i ← 0
for s ∈ {x^2 mod 4n : x ∈ Z_{4n}} do
  if 2|s then
    B ← {b ∈ Z_n : 2 | b}
  else
    B ← {b ∈ Z_n : 2 ∤ b}
  end if
  for b ∈ B do
    c ← (b^2 − s)/4 mod n
    P[i] ← {x^2 + bx + c}; i++
  end for
end for
return P
```



References

Stangl, W. D. (1996). Counting Squares in $\mathbb{Z}_n$. *Mathematics Magazine*, 69(4), pp. 285-289. https://doi.org/10.1080/0025570X.1996.11996456

Nagell, T. (1964). *Introduction to Number Theory* (2nd ed.). New York: Chelsea Publishing Company.

Acknowledgements

Thank you to Michael Monagan for his supervision and contributions.